AD_____

Award Number: W81XWH-09-2-0013

TITLE: Research and Development for Advanced Tele-maintenance Capability with Remote Serial Console Access and Proactive Monitoring of Medical Devices

PRINCIPAL INVESTIGATOR: David Van

CONTRACTING ORGANIZATION: Concepteers LLC
Jersey City, NJ 07306

REPORT DATE: September 2009

TYPE OF REPORT: Final

PREPARED FOR: U.S. Army Medical Research and Materiel Command
Fort Detrick, Maryland 21702-5012

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
09-15-2009	Final	02-15-2009 to 08-15-2009

4. TITLE AND SUBTITLE
Research and Development for
Advanced Tele-maintenance Capability with Remote Serial Console Access and Proactive Monitoring of Medical Devices

5a. CONTRACT NUMBER
W81XWH-09-2-0013

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

David Van
Email: dvan@concepteers.com

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Concepteers LLC
880 Bergen Avenue, Suite 403
Jersey City, NJ 07306

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
US Army Telemedicine and Advanced Technology Research Center
504 Scott Street
Ft. Detrick, MD 21702
Mr. Tony Story

10. SPONSOR/MONITOR'S ACRONYM(S)
TATRC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an office Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
The U.S. Army Medical Department has the urgent need of a remote diagnostic access (RDA) capability in support of the configuration, problem detection, and troubleshooting of medical equipment densities within the theatre of operations and in fixed medical facilities throughout the world. Currently, there is no telemaintenance capability for medical equipment. Through research efforts funded by U.S. Army Telemedicine and Advanced Technology Research Center (TATRC) and the US Army Medical Materiel Agency (USAMMA), the objective is to develop a comprehensive RDA in support of telemaintenance. The research concluded with a cost effective prototype device that enables biomedical technicians to perform secure remote diagnostics. The new RDA capability supports both in-band and out-of-band console access allowing the technicians to effectively and efficiently perform secure remote diagnostic tasks. The key achievements of the research includes the engineering of the RDA prototype device that is agnostic to the brand, make, or model of the medical equipment; and a unique ability to support remote USB Smartcard, which remotely unlocks the diagnostic functions on the medical equipment. The new RDA capability improves the availability and resilience of the medical equipment, reduces costs associated with unscheduled repairs, and validates equipment performance measures, which in turn provides the physicians with the ability to deliver quality health care to their patients.

15. SUBJECT TERMS
Telemaintenance, Remote Diagnostic Access (RDA), Serial console, USB console, Remote USB Smartcard, Over-the-shoulder, in-band and out-of-band maintenance

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					David Van
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU	54	**19b. TELEPHONE NUMBER** *(include area code)*
U	U	U			646-932-6459

Standard Form 298 (Rev. 8-98)
P ib d b ANSI Std Z39 18

TABLE OF CONTENT

	Page
INTRODUCTION	**4**
BACKGROUND	**6**
ANALYSIS AND CHALLENGES	**12**
MILESTONES AND APPROACHES	**15**
KEY RESEARCH ACCOMPLISHMENTS	**25**
EVALUATIONS AND REPORTABLE OUTCOMES	**27**
CONCLUSION	**39**
REFERENCE	**41**
APPENDIX I – SERIAL COM PORT REDIRECTOR	**42**
APPENDIX II – INTRODUCTION TO PKI / CAC	**46**

INTRODUCTION

The U.S. Army Medical Department has the urgent need for a remote diagnostic access (RDA) capability and a proactive monitoring system in support of the configuration, problem detection, and troubleshooting of medical equipment densities within the theater of operations and in fixed medical facilities throughout the world. In 2008, the U.S. Army Medical Materiel Agency (USAMMA), with support from the Telemedicine & Advanced Technology Research Center (TATRC), established a multi-phase research and development initiative to establish a new telemaintenance platform for its medical equipment maintenance operations. The new platform consists of two key objectives: the RDA capability to enable secure remote access for medical equipment diagnostics, and the Proactive Monitoring capability to enable early problem detection by leveraging the new RDA capability. Considering the RDA capability as "paving the roads" on which diagnostic activities and equipment statistical information can be transported, then the Proactive Monitoring capability can be viewed as "problem sensors" for early problem detections. Being able to detect impending equipment problems before they occur is the beginning of a transformation from the current time-based maintenance methodology to a condition-based maintenance (CBM+) operations model. All of these are fundamental building blocks of the telemaintenance platform; furthermore, they align with the requirements and objectives of the Hospital of the Future (HOF) initiatives as well.

The subject of this report is the research, evaluation, development, and demonstration of the new RDA capability as the foundation of the new medical equipment telemaintenance platform. This scope of the research is to develop a unified remote diagnostic access gateway with an efficient methodology for provisioning secure remote access for medical equipment diagnostics. This unique RDA gateway provides all the necessary tools to enable proprietary and legacy medical equipment, including those without native RDA support, to become telemaintenance-ready. The new methodology provides technicians with the ability to remotely perform diagnostic tasks and resolve problems without any time and physical constraints. With such a new RDA capability, a

local maintainer can collaborate with subject matter experts (SMEs) via the "over the shoulder" view of the medical device; or a remote technician can "reach in" via secure access to calibrate machine components, retrieve error logs, or upgrade configuration files – all of which can be achieved through an extensive set of RDA functions that are agnostic to the brand, make, and model of the failing medical equipment.

This report encompasses findings and results pertaining to the RDA phase of the medical equipment telemaintenance initiative. The research on Proactive Monitoring is the second phase of the research and is underway. Filings and results for the Proactive Monitoring research will be reported separately. The purpose of the current RDA research is to improve the availability and resilience of the medical equipment, reduce costs associated with unscheduled repairs, and validate equipment performance measures, which in turn provides the physicians with the ability to deliver quality health care to their patients. The second phase of the research will focus on enabling condition-based maintenance and its transformation from a time-based maintenance operations model.

BACKGROUND

The current medical equipment maintenance model is “on site and physical”, rather than “remote and virtual”. There is no comprehensive nor standardized RDA capability for biomedical technicians to troubleshoot and resolve problems remotely and securely. Additionally, the current operations model is “reactive”, rather than “proactive”, in terms of early problem detection and prevention. The lack of visibility to the health of medical equipment and the need to be on site for problem resolution, coupled with frequent rotations and scarcity of medical equipment technicians, continue to cause considerable downtime of critical medical equipment densities and is detrimental to the health care support to our war fighters.

Complex medical equipment such as Magnetic Resonance Imaging (MRI), Computed Tomography (CT), Computed Radiology (CR) scanners, along with ultrasonic and laboratory devices are critical to the patients’ treatment regimen. Unscheduled delays and/or extensive downtime of the equipment severely hamper the physicians’ ability to diagnose and treat a patient’s injury or medical condition. Complexity often requires the local maintainer to rely on external support or SMEs, many times from the equipments’ manufacturer, to assist in the diagnosis and repair. This “wait and see” method coupled with the lack of any prescreening capability to identify troubled areas, worn parts, or signal “out of tolerance” modalities can cause additional delays.

While medical equipment manufacturers offer variations of managed-services to monitor and maintain medical equipment in service for commercial installations, these offerings often can only support individual manufacturer’s own brand and model of medical equipment. Furthermore, their service architecture and the providers’ infrastructures generally do not comply with the government’s security protocols and regulations. As a result, virtually all the offerings do not have the authority to operate (ATO) within the government networks due to the lack of accreditations and compliances. Compounding the problem is the fact that manufacturers are reluctant to release proprietary hardware and software specifications, access protocols, application

programming interfaces (API), or software development kit (SDK) to allow independent development, integration, and support for telemaintenance in medical equipment operations.

An earlier attempt was made to implement RDA capability for medical equipment using teleconferencing tools that worked effectively for telemaintenance of aircrafts and vehicles. This type of system is generally made up of a video camera, an audio device (microphone, speaker, or handset), a computer with pre-installed diagnostic software, a communication device for network connectivity (wired, WIFI, satellite link, etc.), and an optional battery for mobility. The system utilizes video for remote over-the-shoulder viewing during troubleshooting hardware failures, and the audio gears allow the local maintainer to communicate with the remote SMEs. When the system was used in medical equipment telemaintenance, the RDA capability provided by the system was found to be inadequate. Some of the limitations are:

1. In general, medical equipment troubleshooting requires proprietary diagnostic software supplied by the equipment manufacturer and they must run on the local maintainer's laptop. The software also requires a physical serial cable connecting from the laptop to the medical equipment's console port (a DB9 port is common although newer equipment comes with a USB port instead). Since the software is very specific to the brand, model, and firmware versions of the medical equipment being diagnosed, the local maintainer must use the software that matches the hardware component to ensure compatibility. This means, if the teleconference system is used for medical equipment telemaintenance, the computer found in the system must have all the diagnostic software pre-installed, including different version of the same software. Even if it is possible to pre-load all the diagnostic software from all the manufacturers into all the teleconference systems' computer, it is impossible to keep the versions of all software up-to-date on these systems.

2. The teleconference system is usually equipped with one serial port to support wired console access. This means the local maintainer cannot diagnose several

equipments simultaneously, or he cannot efficiently troubleshoot on complex equipment with multiple console ports, such as the MRI.

3. The teleconference system is designed for on-demand applications. That is, a local maintainer would connect this device to the medical equipment at the time of need – when the equipment needs repair. This method is not a long-term solution given one of the medical telemaintenance's objectives is the proactive monitoring capability, which would require the teleconference system to have a persistent connection to all the medical equipment being monitored.

Another previous attempt to establish RDA for medical telemaintenance was the use of conventional access solution designed for telecommuters and tele-supporters in the Information Technology (IT) world, such as a virtual private network (VPN) and other secure access gateways. This type of solution enables a remote user to connect to a computer at the office, or allows an IT support personnel to remotely access the user's computer to troubleshoot a software issue. When the solution was tested for medical equipment telemaintenance, it was also proven inadequate. The limitations are:

1. Telecommuter systems (hardware, software, or both) are in-band or network-based access solution. They work effectively when the remote computer and its operating system are healthy. This type of solutions generally does not provision access for out-of-band methods, such as serial console, universal serial bus (USB) console, or keyboard video mouse (KVM) consoles. For medical equipment diagnosis or calibrations, out-of-band access method is required. As such, out-of-band access devices must be added to the in-band access solution. The resulting RDA solution becomes very bulky and difficult to manage, as explained below.

2. Conventional IT-centric access solutions are generally not designed for medical operations environment, such as the ER, mobile hospitals, and etc. First, the hardware form factor is designed for mounting on a rack. For medical equipment

telemaintenance, the form factor should be miniaturized so that the access device can be embedded inside and become an integral part of the medical equipment.

3. Commercial off the shelf (COTS) products for out-of-band access are available, such as those serial-over-LAN devices designed for Supervisory Control And Data Acquisition (SCADA) applications, and KVM-over-LAN for headless server applications. This method of bundling different brands of out-of-band devices, with each one being a stand-alone or point solution, to create the RDA capability for medical equipment telemaintenance is not ideal because it is impossible to integrate all these COTS products into a single management point.

In order to understand the issues pertaining to RDA for medical equipment telemaintenance, the next few sections summarize various subjects that are relevant to the research approach and prototype strategy to be discussed later in the report:

- **In-band and Out-of-band RDA for Medical Equipment**

In-band access is a "network-based" access method, which allows a technician to access the medical equipment via the network. This implies that the Operating System (OS) and the access application servers running on the OS in the medical equipment, such as the Virtual Network Console (VNC) server, File Transfer Protocol (FTP) server, Secure Shell (SSH) server, etc., must be fully functional.

Whenever the medical equipment is having a problem at the OS or firmware level (hardware), the network services supporting remote access often become unavailable; and consequently, the equipment can not be reached via the network. This is because the network driver and the associated services are not running when the OS is not operational.

Out-of-Band is a "non-network" access method, which allows the technician to access the medical equipment using a physical connection between the user and the console found on the equipment. The console port can be one of three types: serial (DB9,

DB25), USB, and KVM. Universally, the purpose of the console port is to allow administrative access for configuration, troubleshooting, or calibration when the equipment is either not accessible via its network interface; or in some cases, certain administrative tasks can only be performed via the console. The term "console access" is analogous to an out-of-band access.

- **Understanding Console Access for IT Operations**

In IT operations, network and server administrators typically use in-band access to perform routine maintenance tasks while the device is fully functional. However, for configuration changes or when the device is non-functional due to component failures, they must rely on the out-of-band or console access to configure and troubleshoot the problem.

A network technician generally uses a serial console access method for their remote diagnostic access. One thing to note is that the serial console access in the IT world has been standardized such that the software used to connect to a serial console on one brand of network router is the same for accessing the console on another brand; furthermore, the same software can be used to connect to the serial console on different brands of server. Specifically, the common protocols are Telnet and SSH for "terminal emulation access", the actual implementations are known as reversed-Telnet and reversed-SSH, respectively.

Another standard in IT operations for serial console access is the use of a serial console server, a device that accepts the user's commands via the network protocols and then relays the messages to the console on the device via a serial communication protocol. With this device, along with the standardized access protocols, remote diagnostic access capability for IT operations, even for out-of-band access, have been achieved and is a common practice.

A new type of serial console, based on the USB standard, appeared in recent years. The USB console access method is completely different from the serial console and it is still

uncommon even for IT practices. The remote diagnostic access for IT equipment, based on the USB console access method, is almost non-existent.

A server administrator generally uses a network-enabled KVM console access method to remotely maintain servers. The KVM console is simply a device that takes the analog video output signals from the VGA port on the server and converts it to digital signals so that they can be transmitted over the network. The KVM console allows the administrator to take control of the server hardware (with the ability to control the mouse and keyboard while viewing the monitor output) as if he / she is physically in front of the server. The KVM access method used in IT operations is well established and can support virtually all hardware and OS platforms.

ANALYSIS AND CHALLENGES

Initial site surveys and evaluation of medical equipment at the Army Depot in Tobyhanna PA, the FEMA depot at MD, and the US Army Medical Center in Landstuhl Germany, along with interviews with Army medical maintenance personnel, indicated the following conditions and challenges:

1. Medical equipment uses many different types of in-band and out-of-band access methods for maintenance and troubleshooting.

   Challenges:

   a) Develop a method to easily quantify all the possible access methods so a comprehensive RDA capability can be defined.

   b) Identify a COTS product as a baseline for the RDA gateway that can support both in-band and out-of-band access methods in a single device.

2. A majority of medical equipments' diagnostic method uses the serial COM port which necessitates a physical serial cable between the technician's laptop and the equipment; and proprietary diagnostic software is needed to communicate with the equipment's firmware. (See Appendix I for more information on Serial COM Port Redirector.)

   Challenge: Implement a method of serial console access that is different than the standardized method commonly used for RDA in IT operations.

3. A majority of new medical equipment are switching from the serial console port to a USB console port.

   Challenge: Develop a RDA feature using USB-based console access method which is uncommon even in IT operations.

4. Some manufacturers, such as Philips, implemented physical security via a USB Smartcard to unlock administrative / diagnostic functions in their medical equipment. For example, in order for a technician to perform diagnostic tasks on the Philips Eleva Workstation, a component of the Philips CR System, a USB Smartcard supplied by Philips must be physically inserted into a USB port on the workstation in order to unlock and access the administrative features in the system software.

   Challenge: Develop a technology that can virtually insert the USB Smartcard into the medical equipment when the remote technician physically inserts the USB Smartcard into his/her laptop.

5. Network connectivity in certain Army medical operations, such as mobile hospitals in theater, is limited or unavailable. It may be difficult to connect a RDA gateway to the site due to the lack of available Ethernet wiring.

   Challenge: The RDA gateway must be equipped with a wireless network interface to support the Army's Combat Service Support Automated Information System Interface (CAISI V2) as an alternative or backup network connection.

6. The hardware form factor of the RDA gateway must be miniaturized due to the lack of server rack in virtually all medical operating environments.

   Challenge: Identify a suitable COTS hardware platform that can support all the RDA functions, but at a fraction of the size of a conventional access gateway used by IT operations.

7. The RDA gateway can be perceived as an IT access device. As such, it must comply with the Federal Information Processing Standards (FIPS 140-2) for the encryption function provided as part of the RDA capability.

Challenge: There is no known FIPS compatible or certified COTS console access device on the market, that has the small form factor, sufficient hardware resources (CPU, memory, storage), and multiple built-in serial and USB console interfaces.

8. The RDA gateway has to provide unobstructed connectivity between the technician, or SMEs from the manufacturer site, to the medical equipment inside the Army network. As such, the RDA gateway must comply with the DoD Ports, Protocols, and Services Management Program (PPSM).

Challenge: Globally encapsulate all the different network ports, necessary to support all variations of RDA methods, using the Secure Sockets Layer (SSL) protocol such that all RDA activities are fully encrypted and only a single transport TCP port is used.

9. The RDA gateway has to support authentication based on Public Key Infrastructure / Common Access Card (PKI / CAC). (See Appendix II for an introduction to PKI/CAC)

Challenge: Identify a COTS product that is small enough for medical RDA application with a sufficient processor that can support this resource-intensive authentication method.

10. The medical operations network is usually segmented and isolated from the production IT networks. Given the numerous enclaves and complexity of the government network, the RDA gateway must support different methods of routing, inclusive of packet forwarding, bridging, and network address translation (NAT) in order to ensure the interoperability of the gateway within the various network topologies of DoD.

Challenge: Identify a COTS product as a baseline for the RDA gateway that can natively support all these routing methods.

MILESTONES AND APPROACHES

Milestone 1A: Develop a method to easily quantify all the possible access methods so a comprehensive list of RDA capability can be defined.

Approach: To discover all the possible access methods employed by medical equipment manufacturers, a test lab was established at an MC4 facility in MD to conduct the research. The lab was populated with a sample of medical equipment, all of which have no native support for telemaintenance. These equipment were obtained from the Army Depot at Tobyhanna PA and vendors. The following is a partial list of the surveyed medical equipment:

Philips Compano CR Reader
Philips Eleva Workstation
Philips Easy Vision
AccuTemp HemaCool
Fujifilm CR Viewer
Fujifilm CR Printer
Miscellaneous lab equipment

Additionally, evaluations and site surveys were conducted at the Army Depot in Tobyhanna PA, the FEMA depot at MD, and the US Army Medical Center in Landstuhl Germany. Complex equipment tested included:

Philips CT MX8000
Toshiba CT
MRI components
C-Arm
Miscellaneous portable sensors (oxygen tank, etc.)

Biomedical Technician and Depot Personnel interviewed:

Mr. Mark Mills
Various Maintenance personnel at Tobyhanna Army Depot

Result: Success.

The discovery process established a RDA Matrix that can be use to classify medical equipment based on their access methods. The following table represents a unified RDA capability that can support the majority of medical equipment, and it serves as the foundation for the new medical equipment telemaintenance platform:

RDA Capability Matrix

Code	Access Method	Applications	Description
IB001	In-band Port Tunnel	Over-the-shoulder	Network-based RDA for UltraVNC, RDP, software with static network ports
IB002	In-band VPN	File Transfer	Network-based RDA for FTP, and software using dynamic network ports
IB003	In-band Bridging	Proprietary handshake used by some manufacturers	Network-based RDA for proprietary software and network protocols
OBS001	Out-of-band Serial Console Emulation	Accessing equipment serial console using standard text- based emulators	Serial console session uses standard term emulator software such as VT100 (same RDA method for IT operations)
OBS002	Out-of-band Serial Console Virtual COM	Accessing equipment serial console using proprietary diagnostic software	Serial console session uses virtual COM port and network encapsulation for remote access
OBU001	Out-of-band USB Console	Accessing equipment USB console using proprietary diagnostic software	USB console session Uses virtual USB Device driver and network encapsulation for remote access
OBK001	Out-of-band KVM	Accessing equipment KVM console	KVM console access over the network

OBK002	Out-of-band KVM Remote Smartcard	Accessing equipment KVM console that requires USB Smartcard to unlock admin/ diagnostic functions	KVM console access with the unique capability to forward the Smartcard credential from technician laptop to the remote medical equipment

Milestone 1B: Identify a COTS product as a baseline for the RDA gateway that can support both in-band and out-of-band access methods in a single device.

Approach: COTS access solutions, made for IT operations, can only support either in-band or out-of-band access method. They seldom support both because the market for in-band access is different from the out-of-band access market. As such, our ability to evaluate the COTS products meeting this requirement was limited. The research efforts identified only a few vendors offering products that can support both in-band and out-of-band access methods. However, to qualify for the small form factor (see milestone 9 below), only a single product was found to be small enough and can support both in- and out-of-band methods.

The research team first evaluated the COTS product with the medical equipment in the lab, and consequently compared the list of supported access methods against the matrix. Although it can only support access codes IB001, OBS001, and OBS002; the research team was able to obtain the firmware source code from the product manufacturer and modified it to add access code IB002 and OBU001. Concurrently, the research efforts also identify another COTS product to support access code OBK001 (see Milestone 4 for additional information). The second product would be an add-on module to the first as a prototype RDA solution for medical equipment telemaintenance.

Result: Failure

Even though the two COTS products were extensively modified and enhanced by the research team, and the final prototype solution was able to support almost 100% of all the

access methods in the matrix, the first product was eventual discarded because it failed to satisfy the following milestones:

Milestone 5 failure– there's no support for wireless connectivity. It was impossible to add a wireless network in the ultra small form factor.

Milestone 7 failure – Because the product uses an Arm processor, there is no known Arm-based access product on the market with a successful FIPS certification. The research team consulted the experts on FIPS accreditation and was told it would be a major undertaking.

Milestone 9 Failure- The Arm processor and the limited embedded flash memory were insufficient to process and store the massive PKI/CAC database. If the product cannot support DoD's PKI/CAC authentication method, it will fail the Defense Information Systems Agency's (DISA) Joint Interoperability Test Command (JITC) accreditation for PKI/CACAuthentication in the future.

Resolution: Success

The research team consulted with custom hardware manufacturers and developed a new prototype utilizing COTS embedded computer components. The new prototype device has all the hardware interfaces necessary to support all the access code, working in conjunction with an external module that provides for OBK001 and OBK002. Additionally, it has a more powerful processor to satisfy the requirements of milestones 5, 7, and 9.

Milestone 2: Implement a method of serial console access utilizing a virtual COM port and network encapsulation to eliminate the serial cable.

Approach: A medical equipment technician needs to use a serial cable to connect his/her laptop to the serial port on the medical equipment for access. Once the serial connection is established, the technician launches the proprietary diagnostic software,

supplied by the manufacturer to work with specific model equipment, to perform diagnostic, configuration, or calibration tasks. The significance here is that the software, running on the technician's computer, is actually using serial communication to send and receive messages to and from the medical equipment. This method of connectivity, along with the serial-based communication, necessitates the technician to be on site to do the work.

To achieve RDA capability, the research team looked to a proven remote diagnostic access method that can be adapted to support medical equipment. It is the Supervisory Control And Data Acquisition (SCADA) infrastructure. In the utilities and manufacturing industries, there exists a product known as the serial device server. The purpose of the serial device server is to extend the serial communication from the software, running on the SCADA operator's computer, to the serial port on the assembly machine. The process is to first create a virtual communication (COM) port on the user's computer to simulate a COM port that the software needs to communicate with. Next, a specialized network driver, running on the same computer, wraps all messages, from the software to the COM port, inside a network packet. The packet is then being transmitting to the serial device server located in some remote site. Finally, the serial device server receives and unpacks the packet; and sends the raw serial messages to the machine via the serial cable wired to the serial device server. The process is reversed for transmit messages from the machine back to the software on the operator's computer.

Result: Success

The research team developed the virtual COM software and integrated this new function into the prototype device. This new function was tested with all the medical equipment in the lab that traditionally requires a serial cable to work with the proprietary diagnostic software. The result was remote accessibility to equipment with no native telemaintenance function.

Milestone 3: Develop a RDA feature using a USB-based console access method which is uncommon even in IT operations.

Approach: Similar to milestone 2, the USB console access method in the RDA capability requires a universal USB driver that simulates another USB driver such that the proprietary software can detect the presence of a USB connection to the medical equipment.

The difficulty in implementing this access method stems from the fact that USB console is a new generation of portal for diagnostic access. Even IT operations currently do not utilize this type of console access. The research team found only one COTS product on the market that advertised such a capability. However, after a thorough evaluation of the product, it was determined that the product is problematic and the driver and software utilities are of beta-quality. The product manufacturer was unable to resolve reported crashes experienced during our evaluation.

The research team identified a software-based USB-over-LAN solution designed for 3rd-party integration, rather than a COTS production. After extensive collaboration with the software vendor, the research team was able to integrate a licensed software module and successfully tested remote access to remote equipment using the USB console access method.

Result: Success

Milestone 4: Develop a technology that can virtually insert the USB Smartcard into the medical equipment when the remote technician physically inserts the USB Smartcard into his/her laptop

Approach: To accomplish this specific requirement, the research team had to look to a relatively new technology that is being used in IT operations. The technology is known as "virtual media". The virtual media feature is designed to allow an IT support engineer to

perform a “bare-metal” administration or reconstruction of a remote server. This feature virtualizes the media in the engineer’s possession, such as a CD image, a physical CDROM, or another type of storage device, to become accessible by the remote server. With it, the engineers can re-load the OS or firmware on the remote server via an out-of-band access method.

The research team first identified a COTS product that has a built-in virtual media capability. After joint research and development, the manufacture was able to enhance the product’s original virtual media function to also forward the smartcard credentials over the network.

With the new firmware loaded on the COTS product, and a new virtual smartcard driver integrated with the RDA gateway, the research team conducted numerous tests in the lab with successful results: by inserting the USB Smartcard into a laptop that has an active connection to the RDA gateway, the USB Smartcard is virtualized and the remote medical equipment was able to detect the security device as if it was physically inserted into the equipment at a remote site. Consequently, this process unlocked all the administrative/diagnostic functions on the medial equipment.

Result: Success.(See section 1 in the Evaluation and Reportable Outcomes section for the actual test report)

Milestone 5: The RDA gateway must be equipped with a wireless network interface to support the Army’s Combat Service Support Automated Information System Interface (CAISI V2) as an alternative or backup network connection.

Approach: The new custom hardware developed for milestone 1B has a built-in wireless network interface (IEEE 802.11n). Upon review of the Army CEISI V2 ATO, the research team implemented the necessary drivers to support the WI-FI Protected Access (WPA-2) standard.

The prototype RDA device was able to successful connect to the Army CAISI V2 wireless access point (AP) at the MC4 facility in MD.

Result: Success .(See section 2 in the Evaluation and Reportable Outcomes section for the actual test report)

Milestone 6: Identify a suitable COTS hardware platform that can support all the RDA functions, but at a fraction of the size of a conventional access gateway used by IT operations.

Approach: This milestone was achieved as part of the resolution for milestone 1B. (See milestone 1B, resolution section for more detail).

Result: Success

Milestone 7: There is no known FIPS compatible or certified COTS console access device on the market.

Approach: This milestone was achieved as part of the resolution for milestone 1B. The implementation of FIPS-compatible encryption for all RDA network traffic is through the use of the FIPS 140-2 certified cryptographic module / library from OpenSSL.org. By utilizing a specific version of the library without any change made to the source code, the process is known as "self validation" as defined by the terms of use for the OpenSSL source code. Upon self validation, the RDA prototype device can operate in FIPS and non-FIPS mode.

Result: Success

Milestone 8: Globally encapsulate all the different network ports, necessary to support all variations of RDA methods, using the Secure Sockets Layer (SSL) protocol such that all RDA

activities and information exchanges between the technician and the medical equipment are fully encrypted and only a single transport TCP port is used.

Approach: As part of the FIPS compatibility implementation, all ingress and associated egress network traffic are encapsulated using the SSL protocol. As such, regardless of the native network ports used by various access methods supported by the RDA prototype device, for in-band as well as out-of-band access methods, a single transport port is used (TCP 443). This ensures that routing of RDA activities in DoD enclaves complies with the DoD PPSM.

Result: Success

Milestone 9: Identify a COTS product that is small enough for medical RDA applications with a sufficient processor that can support the resource-intensive PKI/CAC authentication method, which also relies on a Lightweight Directory Access Protocol (LDAP) infrastructure inside the RDA gateway.

Approach: The new custom hardware developed for milestone 1B utilizes Intel's latest Atom-series CPU which is many times more powerful compared to the Arm processors commonly found in COTS serial device server products. With the new form factor, memory and storage capacities have been significantly increased to sufficiently handle the large database of DoD credentials.

The prototype RDA device was able to successful authenticate with JITC's PKI/CAC test portal, utilizing a JITC distributed CAC.

Result: Success

Milestone 10: Identify a COTS product as a baseline for the RDA gateway that can natively support all these routing methods.

Approach: In order to support all type of network routing schemes, to ensure interoperability of the RDA gateway with DoD's network enclaves, the research team implemented three types of VPN: Packet Forwarding, Network address translation, and bridging. The allows the RDA gateway to be compatible with virtually all known remote access network topology designs.

Result: Success

KEY RESEARCH AND ACCOMPLISHMENTS

Technology

- Developed a unique prototype device to unify and simplify the deployment of the RDA capability across all US Army Medical operations.

- Developed a unique Remote USB Smartcard capability to enable RDA by virtually inserting the USB Smartcard.

Methodology

- Established a matrix to quantify all RDA methods necessary to achieve a medical equipment telemaintenance platform objective.
- Developed an effective method to transform any medical equipment to become "telemaintenance ready" by classifying and retrofitting individual equipment based on the RDA matrix.
- Established a telemaintenance platform with a standard for RDA authentication, authorization, and access (AAA) for medical equipment operations.

Integration

- Developed a method of hosting and on-demand distribution of software and drivers to support all RDA methods. This eliminates the need to pre-install software tools or drivers on the technician's government supplied laptops / desktops.
- Consolidated hardware and software components and miniaturized the form factor to create a unique all-in-one RDA gateway.

Interoperability

- Implemented PKI/CAC for RDA to comply with DISA JITC authentication requirements
- Encapsulation of all RDA methods in SSL to comply with DoD PPSM

- Developed a RDA capability that is agnostic to brand, make, and model of the medical equipment

EVALUATIONS AND REPORTABLE OUTCOMES

The research team conducted numerous formal and informal tests, along with evaluations of COTS products in the lab located at a MC4 facility in MD. The following sections detail some of the actual tests conducted with Tobyhanna Depot and MC4 personnel.

Evaluation 1: Remote USB Smartcard Support for Philips Medical Equipment

Background

Remote Diagnostic Access (RDA) is one of the capabilities of Telemaintenance that enables technicians to securely and remotely access, diagnose, and resolve medical equipment issues without the need to be on site.

In previous tests, we used a Philips CR System consisting of the Compano CR Reader (PCR), the Easy Vision Workstation, and the Eleva Workstation. We demonstrated the capabilities of the prototype RDA device (Tele-Console) by provisioning different types of access methods for the technician to remotely access the various components of the Philips CR System, such as the serial console access to the PCR and the keyboard-video-mouse (KVM) console of the Easy Vision and Eleva Workstations. Additionally, we successfully demonstrated support for in-band access methods (network-based services such as Ultra-VNC, Microsoft RDP, PC-Anywhere, etc.). During the tests, the technician was able to remotely access the entire Philips CR System, which has no native RDA support. In conclusion, our prototype RDA device successfully and unobtrusively retrofitted the Philips CR System and made it RDA-enabled.

The Challenge

While the technician was able to remotely access all the components of the Philips CR System, there was one condition in which the technician was unable to perform all the diagnostic tasks on the Eleva Workstation. This particular device required the technician

to be on site to physically insert a USB Smartcard into the Eleva Workstation in order to be authenticated and authorized to perform administrative functions. While this was a good security measure on Philips' part, it was detrimental to our RDA-enablement efforts – what good is it if the technician can view the Eleva Workstation remotely but cannot perform any diagnostic tasks unless he goes on site to insert the USB Smartcard?

The Solution

Through our research and development efforts, we have prototyped a unique method of virtualization for the USB Smartcard: through the use of a customized COTS KVM switch, we modified the firmware and added a new function to transmit the USB Smartcard credential from the technician's laptop to the Eleva Workstation. This effectively renders the Eleva Workstation into thinking that a physical USB Smartcard has been inserted to the USB port on the computer.

In preliminary tests, we inserted the USB Smartcard into our test computer and the remote Eleva Workstation successfully detected this USB device.

The Test Setup

Below is the photo of the RDA demo lab in Maryland. The marked equipment in the photo is the Eleva Workstation.

The small photo on the lower right corner is the Philips USB Smartcard (Cardman 6121). This USB "dongle" is usually inserted into the USB port in the front of the Eleva Workstation. The line illustrates the USB port for the Smartcard.

The Tester

Mr. Mark Mills from USAMMA was the technician that conducted the RDA test from Tobyhanna PA. He attempted to use this government supplied laptop and a Philips assigned USB Smartcard with his credential to securely and remotely access the Philips CR System for diagnostic purpose.

The Test Steps

To initiate RDA access to this lab, please start a browser and enter the following url:

1. Https://demolab1.concepteers.com
2. At the login screen, enter the following login / password: XXXX / XXXX

3. Upon successful authentication, you should see the following access screen. This is the default user interface of the prototype Tele-Console (the same unit you took to Iraq):

Description of the screen:

1. Left icons represent the medical equipment in the lab.
2. On/Off is currently inactive. They will allow turning on and off individual equipment remotely when we are done with the implementation.
3. All icons to the right of the On/Off box represent accessible methods to each equipment:
   a. The serial console icon launches a text-based console to the device.
   b. The KVM-App launches a graphical console to the device (out-of-band graphical)
   c. The RDP icon launches a remote desktop to the device (in-band graphical mode)

NOTE: As this is an active development / testing environment, certain equipment have not been configured for full access. As such, and for the purpose of testing the Remote USB

Smartcard key virtualization (forwarding the credential from your PC to the Eleva Workstation), please follow the steps in the next page.

Test Procedure

Preparation: Ensure that the Philips USB Smartcard (dongle) is inserted into your computer, and that your system can recognize it.

Connection: Launch a browser and login to the Tele-console at the Maryland lab as previously described.

Accessing the Eleva Workstation: Click on the "KVM-App" icon for the Eleva Workstion (2nd from the top).

NOTE: The Eleva Workstation of this Philips CR System came from Tobyhanna so it is one of "your" medical equipment.

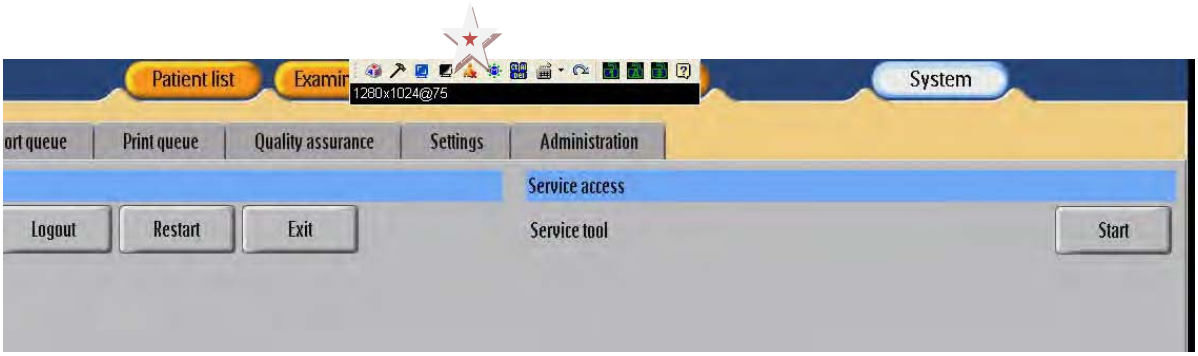
A client will be downloaded to your computer. Use the account credential to fill in the popup login screen (if necessary):

Click Login. You should soon see the "Remote View" become active. Please click on the Remote View button.

The screen of the remote Eleva Workstation will soon appear on your monitor. You now have full remote Keyboard and Mouse control as if you are in front of the machine in person.

The current login session is with account "eleva" and password "eleva". Please logoff and login using your own account that matches your smartcard credential, if necessary.

To test the remote USB smartcard capability, you have to activate the virtual smartcard function. In the screenshot below, there is a menu on the top of the remote session as show in the screenshot below:



Click on the 5th icon from the left (marked with star above) to initiate virtual media (for remote smart card).

When a popup window appears, you can select the Cardman 6121 from the list of detected devices. Once you click the Start button, the remote Eleva Workstation will detect your USB Smartcard as if it is locally inserted.

At this point, you can proceed with your administrative access and test the effectiveness of this new remote USB smartcard capability.

Test Conclusion and Feedback

Below is the actual feedback and validation from Mr. Mark Mills.

From: Mills, Mark A Mr CIV USA MEDCOM USAMMA [mailto:Mark.Mills@amedd.army.mil]
Sent: Friday, June 19, 2009 7:42 AM
To: dvan@concepteers.com; Poole, Elizabeth A Ms CTR USA MEDCOM USAMRMC
Cc: jchi@concepteers.com; Rosarius, Jack K Mr CIV USA MEDCOM USAMMA; Roth, Terrance Mr CIV USA MEDCOM USAMMA; dvan@concepteers.com
Subject: Re: Testing Remote CR w/USB (UNCLASSIFIED)

Liz

Here's the result of the test.

We started the remote test at 1800 and finished at 2030. I was able to connect to the Eleva using my Philips issued dongle key on my government issued laptop at my end in PA and access the Eleva in Maryland.

I was able to go into the service mode and configure the network settings and access everything I could by being on site, prior to this, it was only possible by being on site and actually inserting the USB dongle into the Eleva workstation.

I also was able to access the CR Reader to pull error code and diagnostic any problem. Every part of the CR system was accessible.

This will be a nice feature if we can add this to the RDA project. I also tested it from my personal desktop computer and it worked great. I can see added value if we integrate this into the Toshiba CT downrange. This will allow us to remote in and actually troubleshoot the RAID on the CT, in case they have any storage issues.
Mark Mills

Evaluation 2: Tele-Console Wireless Connectivity Test to Army's CAISI v2 LAN

Background

Concepteers is developing a remote diagnostic access (RDA) prototype device to enable enhanced telemaintenance capabilities for technicians supporting and maintaining medical equipment in theater of operations. The prototype device, Tele-Console, typically connects to the medical equipment's console port using a serial cable. For remote access, the Tele-Console also needs to be connected to the local area network (LAN) and consequently, be reachable by the technicians from various enclaves of the military network (.mil) or the commercial network (.com). This "reach-ability" is the focus of our tests.

Challenges & Solutions

There are known connectivity challenges, from a technology and its interoperability stand point. That is, we are excluding restrictions and limitation of access motivated by political agenda; this type of challenge can't be addressed by the scope of the research efforts.

The following conditions may be common and are challenges we hope to address:

1. Lack of physical network wiring – unlike an office setting, a mobile hospital in theater may not have available or spare network connections to support RDA.

   The solution is to provide support for wireless connectivity, in the Tele-Console, that can take advantage of Army's Combat Service Support Automated Information System Interface (CAISI v2), which is an Army wireless LAN. Since CAISI v2 will be deployed to 30,000 locations by 2010, interoperability and connectivity with the CAISI is a future-ready capability of the Tele-Console.

2. The CAISI requires specific encryption and authentication protocols in order to allow a device (such as the Tele-Console) to connect to the wireless LAN.

   The solution is to identify COTS wireless adapters that can be integrated with the Tele-Console and can support the WPA2 PSK encryption and authentication methods to comply with the ATO from PEO-EIS.

3. At the CSH, an access gateway may exist, such as the GateKeeper, and is deployed as a perimeter security measure. Until the Tele-Console acquires accreditations from NIST (CC-EAL and FIPS), JTIC, and its ATO, it relies on the accreditations from the perimeter access gateway. The challenge is the interoperability between the Tele-Console and another access gateway device.

   The solution is to engineer the Tele-Console with the appropriate technology and methodology that can co-exist with another encryption tunnel facilitated by the perimeter access gateway. To accomplish this, the Tele-Console has been designed to appear to the other access gateway as a regular device on the network. Once the gateway authorizes a remote technician to access the Tele-Console, with just a single SSL port (443), the remote technicians can gain full access to medical equipment consoles to perform diagnostics procedures.

The solution presents a number of benefits:

1. When the Tele-Console is deployed behind the outer access gateway, all network traffic between the remote technicians and the Tele-Console has dual layer encryptions. This enhances security and protection of data.

2. The interoperability between the Tele-Console and the outer access gateway presents an opportunity for segregation and delegation of access control for IT versus medical equipment. In other words, the management of the outer access gateway is generally the responsibility of the IT / security teams. Since these

management points wouldn't know anything about RDA for medical equipment, the Tele-Console's access management can be assigned to appropriate groups within USAMMA.

3. A traditional access gateway is designed for in-band remote access. The Tele-Console can be viewed as an augmentation or enhancement to the existing gateway because the Tele-Console provides out-of-band or console access to medical equipment.

4. When the Tele-Console device receives all the necessary accreditations, it offers the flexibility of operating as a stand-alone access gateway for medical equipment, or can interoperate with IT's existing access gateway.

Field Test Procedure and Result

On July 8, 2009 at 15:00, Concepteers engineers conducted a wireless connectivity test at the MC4/L3 facility at Key Parkway in Frederick, MD. With assistance from MC4/L3 engineers, Concepteers successfully established a secure wireless connection from its prototype Tele-Console device to the MC4 CAISI v2 Army wireless access point. For the test, the Tele-Console used the WPA2-PSK security and authentication methods to comply with the ATO from PEO-EIS. Below is the detail of the test sequence:

Testing interoperability with GateKeeper

1. MC4/L3 engineer created a test account on the product GateKeeper and configured a new access policy to allow remote access to the Tele-Console on a single SSL port (443).
2. MC4/L3 engineer provided Concepteers engineer the CAISI private SSID, the encryption key, and the authentication method. Concepteers engineer configured the Tele-Console accordingly.

3. Concepteers engineer activated the wireless connectivity feature on the Tele-Console and was able to successfully establish a connection to the CAISI.
4. Concepteers engineer consequently performed "ping test" to confirm the Tele-Console has visibility to other equipments on the CAISI network. The result was successful.
5. MC4/L3 engineer, using his own computer (government supplied and secured), launched a web browser and logged in to the GateKeeper using the test account created for Concepteers.
6. Upon successful authentication, he was authorized to access the Tele-Console. He clicked on the button to launch a connection to the Tele-Console. Subsequently, he saw a login prompt from the Tele-Console.
7. Concepteers provided the MC4/L3 engineer a login account. Upon successful authentication and authorization by the Tele-Console, the MC4/L3 engineers successfully tested access to serial and graphic consoles of the Philips Compano CR, Philips Eleva Workstation, and Fuji CR Viewer Workstation.
8. This concluded the interoperability test.

Note: Because this test was conducted using a DoD-configured computer, we had an opportunity to verify that our method of software distribution, to the user on-the-fly, is compatible and worked successfully with the restrictions of the DoD's security policy.

Testing "Reach-ability" to the Tele-Console in CAISI from the Internet

Because the MC4/L3 computer used in the above test was already in the .mil network, and the Tele-Console, with the wireless connection to the CAISI, is also situated within the .mil network, Concepteers decided to conduct an additional test to verify connectivity to the Tele-Console through the Internet (.com).

1. Concepteers engineer utilized the Verizon broadband service (EVDO) to connect his laptop to the Internet.

2. He launched a web browser and successfully connected to the MC4 GateKeeper device.
3. Upon successful authentication, he was able to successful repeat test steps 3 – 7 above.
4. This concluded the reach-ability test.

Conclusion

Combat Service Support Automated Information System Interface (CAISI) is a tactical wireless LAN located behind DISA's NIPR network and serves as a vital "last mile" connectivity in support of theater operations.

This test validates a new enhanced telemaintenance capability in terms of accessibility to failed medical equipment by remote technicians for timely problem analysis and remediations. With such a wireless capability, RDA no longer depends solely on the availability of physical wiring at individual mobile hospitals in theaters. Since CAISI v2 is expected to be deployed to 30,000 sites by end of 2010, interoperability with CAISI is essential and critical in achieving the RDA objectives.

One possible deployment of the RDA device in mobile hospitals, using wireless connectivity to the Army CAISI V2, involves traversing through DISA's NIPRNet to the LAMC, and from LAMC to the CSH. And from the CSH, there are two possible routes to the Tele-Console:

1. Wired – A physical connection from the CSH LAN to the Tele-Console (not shown).
2. Wireless – A WIFI connection from the CAISI in the CSH to the Tele-Console.

CONCLUSION

Almost a decade ago, in March of 2000, a research was conducted by Logistics Management Institute to survey and provide an overview of the Department of Defense telemaintenance ("Telemaintenance as a process to Increase Maintenance Effectiveness and Efficiency", David M. Cutter, LG903L1). Consequent to that research, in August of the same year, the Air Force Logistics Management Agency conducted its own survey and reported that the survey was unable to identify any ongoing Air Force telemaintenance technology initiatives, and that no one was ever assigned the primary responsibility for telemaintenance related issues ("USAF Telemaintenance Technology Survey", SMSGT Eric J. Mazlik, AFLMA Letter Report LM200020900). Six years later, in March 2006, Air Command and Staff College, Air University, published an update survey report ("An Evaluation of Telemaintenance Capability and Its Impact Within the United States Air Force", Steven A. Oliver, Maj, USAF, AU/ACSC/20-1552/2006). The report stated that the telemaintenance capability within the Air Force has made tremendous progress with demonstrated benefits, effectiveness, and efficiency. The report recommended Air Force to examine its existing methodology and make necessary changes to take full advantage of the new telemaintenance technology.

The above Air Force telemaintenance progress timeline is presented here as a reference to help identify the state of telemaintenance in the US Army Medical Department today, and what can be expected in its own telemaintenance progress timeline.

As a result of this research initiative, with successful development and demonstration of the RDA capability in support of medical equipment telemaintenance, we have proven that the Army Medical Department now has the technology and capability to enable telemaintenance for its operations. However, learning from the Air Force's experience, the newly developed RDA technology from the research efforts absolutely requires a new methodology to become an effective solution. As such, we have the following recommendations:

- Accreditations for the new RDA capability should commence as soon as possible.
- Establish beta sites to thoroughly test the RDA capability.
- Develop a new methodology to retrofit legacy medical equipment in depots so they are telemaintenance-ready, and to evaluate and certify new equipment to be deployed for telemaintenance-readiness.

REFERENCES

1. Nelson, Mark. Serial Communications Developer's Guide. John Wiley & Sons; 2nd Edition, 2000

2. Axelson, Jan. Serial Port Complete: COM ports, USB Virtual COM Ports, and Ports for Embedded Systems (Complete Guide Series). Lakeview Research; 2nd Edition, 2007

3. Pardue, Joe. Virtual Serial Port Cookbook. Smiley Micros, 2007

4. Cappa P, Fedele L. Naso V. A new device for the evaluation of the batteries state of charge. Exp Tech 1999;23(5)

5. Concetti M, Cuccioletta R, Fedele L, Mercuri G. Telemaintenance intelligent systems. Eur Elevator Mag 2005;6

6. Blischke WR, Murthy DNP. Reliability, Modeling, Prediction and Optimization. New York; Wiley; 2000

7. EN 15341, Maintenance key performance and indicators. CEN standard, 2007

8. Wiebe, Michael. A Guide to Utility Automation: AMR, SCADA, and IT Systems for Electric Power. Pennwell Books, 2000

9. Shaw, William. Cybersecurity for SCADA Systems. Pennwell Books, 2006

APPENDIX I: SERIAL COM PORT REDIRECTOR

From Wikipedia, the free encyclopedia

A COM port redirector is a specialized device driver for a Microsoft Windows operating system that includes the underlying network software necessary to access networked device servers that provide remote serial devices or modems.

Overview

The purpose of the redirector is to make the virtual COM port exhibit behavior that closely resembles that of a "real" COM port, i.e., a COM port driver for local serial port hardware. A virtual COM port itself is a relatively simple software mechanism that can be implemented by driver software similar to that of a conventional COM port driver. The main challenges arise in two other areas: the network connection to the device server and the behavior of the device server. These issues are described in the Technology section below.

Applications use a COM port redirector through one or more virtual COM ports that the redirector creates, as configured by the user. When the application opens the virtual COM port, the redirector makes a IP network connection to a device server at a specified IP address and TCP/UDP port number that corresponds to a remote device on the server. The COM port redirector then begins relaying the application data stream between the virtual COM port and the device server.

A redirector will typically permit creation of many (at least 256) virtual COM ports, but simultaneous use of hundreds of ports is often practically limited by a number of factors, including the memory and processor requirements of the redirector, limits on operating system resources, and the performance of the network stack.

A redirector for the Windows operating system is typically configured using a control-panel style graphical user interface for creating virtual COM ports, configuring settings for individual COM ports, and configuring global settings affecting all COM ports. The redirector GUI typically also includes displays of virtual COM port activity and various diagnostic aids.

The performance of a COM port redirector is determined by both its implementation and the network it uses to reach device servers. The performance drawbacks of simple redirector implementations can be largely addressed by kernel-level drivers that avoid context switches. Network packet loss or excessive packet times have dramatic effects on redirector operation and must be avoided.

COM port redirector software products have been offered by at least 30 vendors dating back to the early 1990s. Compatible networked device servers are currently available from a large number of manufacturers, with a heavy concentration of revenue in the top players, who are based in the North America and Asia/Pacific regions.
The equivalent software for a Unix/Linux operating system is commonly called a *tty port redirector* and most of the information on this page applies.

Technology

Redirectors address a number of issues related to the network connection, including:

- Network protocol support that is compatible with the device server.

  Most device servers are accessed with TCP connections (raw or using the Telnet protocol) to gain reliable delivery of the application's data stream in order of transmission. The majority of server manufacturers use public TCP protocols (raw, Telnet, or Telnet with RFC 2217 (http://tools.ietf.org/html/rfc2217) extensions). Several of the larger server manufacturers use proprietary protocols in addition to, or instead of, public protocols. Device servers for certain applications, such as those that use wireless networks, use the UDP instead of TCP to gain performance at the risk of network reliability.

- Initiating the network connection to a device server and determining that server is ready to relay application data.

- Accepting inbound connections initiated by device servers running in *client mode* and routing the data stream to a waiting application.

- Flow control of the network data stream to prevent overrun of the server. (This is not the same as hardware/software flow control of the serial device itself.)

- Data rate limiting of the application data stream to provide the performance expected for the baud rate currently in effect on the virtual COM port, which is slower than the maximum speed of the network connection to the server.

- The timing effects of the TCP protocol stack, e.g. network packetization and the Nagle algorithm.

- Network connections through proxy servers.

- Management of the IP routing table to avoid loss of an IP route to the device server.

- Detection and handling of network interruptions, possibly with an automatic attempt to reconnect to the device server to resume application data flow.

Redirectors must also deal with the feature differences of networked device servers related to:

- Visibility and control of serial line signals such as DSR, DCD, CTS, DTR. The redirector may be able to sufficiently emulate these signals.
- Relay of BREAK signals.

- Settings for hardware or software flow control.

- Handling of the network connection when serial devices or modems disconnect.

Variants

Specialized types of redirectors have been offered to meet the needs of certain applications.

A redirector may support back-to-back operation, in which two computers run copies of the redirector and an outbound connection from one results in an inbound connection to the other. In effect, this technique creates a serial communications tunnel through a network connection. In practice, this configuration works in practice for only certain applications but offers potentially lower costs and higher performance using the Internet to carry serial communications instead of modems between two computers.

A redirector may include a modem emulator that allows the application to use "AT" modem commands even though no physical modem is present. The "number" dialed is an IP address, and the connection is a TCP network connection instead of a modem telephone call. This type of redirector is generally used by applications when originating client software needs to use a modem but the destination for the connection is a network endpoint. Back-to-back operation of this type of redirector can, in some cases, function as a replacement for modems on two computers for some applications. Network effects on timing of the data stream generally preclude the use of this method for transmitting faxes. Additionally, this method is also not reliable if used for PPP connections (such as dial-up networking) due to architectural limitations of the TCP protocol, a topic discussed in technical literature related to TCPover-TCP.

Virtual Serial Port

One variant of a COM port redirector is a Virtual Serial Port. A virtual serial port is a redirector without network software support which is usually used to create a pair of back-to-back virtual COM ports on the same computer. Two legacy applications can then communicate using virtual serial ports instead of conventional inter-process communication mechanisms such as named pipes. Such a virtual serial port is capable of emulating all serial port functionality, including Baud rate, Data bits, Parity bits, Stop bits, etc. Additionally it allows the data flow to be controlled, emulating all signal lines (DTR/DSR/CTS/RTS/DCD/RI) and customizing pinout.

Advantages of Virtual Serial Ports

- Serial port emulation is useful especially when there is a lack of available physical serial ports. Communication between software and/or devices which would otherwise require extra physical connections, can be benefited by using a virtual COM Port emulator.

- Virtual serial ports lets you send or receive data over a TCP/IP port using any serial communication program. This facility allows creating a full-fledged client-server architecture which provides multiple connections and data sharing possibilities between different applications. Such a connection is the best way to allow use of rare and expensive serial devices by different users simultaneously.

- Using serial port emulation one can split a real COM port between a number of virtual serial ports. This makes it possible to supply data from a single serial device to a number of different applications. Such necessity arises when several applications compete for a single GPS connection and the user must close one program to allow another to access a single GPS device.

- A virtual serial port may have the same name as physical one. This facility allows real serial port overlapping (mapping) and receiving data from a physical port through virtual port. In other words, you can map any serial port or virtual port to any other existing port in your system. In this case applications will work with virtual port, but, in fact, they will receive data from overlapped real ports.

Availability

Virtual serial ports are available as both commercial products and free software. Products are available for most recent Windows operating systems, including mobile versions. A free open source virtual serial emulator, namely com0com, can be downloaded from sourceforge.net.

References

- http://constellationdata.com/Network%20Serial%20Port/Network-Serial-Port-Pro-Sdk-Product-Description.asp

- RFC 854 (http://tools.ietf.org/html/rfc854) - Telnet protocol specification

- RFC 2217 (http://tools.ietf.org/html/rfc2217) - COM port control protocol specification

APPENDIX II: INTRODUCTION TO PKI / CAC

By Marek Samulka PhD, Seth Dyer (Concepteers LLC)

The US Government has mandated a Government-wide standard for secure and reliable forms of identification for its employees and contractors. This is being implemented via a Public Key Infrastructure (PKI). A PKI is an arrangement that binds public keys with respective user identities by means of a Certificate Authority (CA), enabling two parties to exchange data securely and privately in what is otherwise an unsecured network.

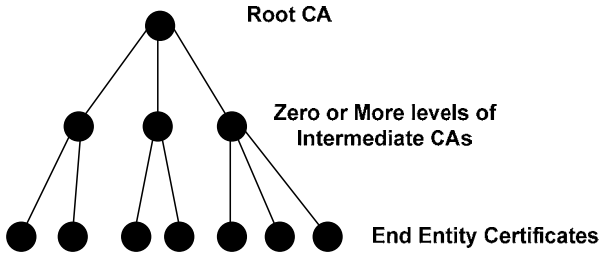
A PKI is built using public key cryptography, which utilizes asymmetric keys. With asymmetric cryptography, everything works off of a key pair. Different keys are used for both encryption and decryption, but they are commutative in nature. Data encrypted with one of the keys can be decrypted with the other resulting in the original data, and vice versa. The owner of the key pair designates one of them as a private key and the other as a public key. The owner keeps the private key safe and can freely distribute the public key for others to easily retrieve it.

There are two main uses for the key pair – encryption and digital signatures. For encryption, the sender converts the data to ciphertext using the receiver's public key. This ensures that only the owner who has the private key can decrypt the ciphertext and view the original data. For a digital signature, the use of keys is the opposite. To sign data, the sender encrypts the data with his/her own private key. The receiver decrypts the ciphertext with the owner's public key. The receiver knows that the data could only be encrypted by the private key, which they trust is only known to the key pair's owner. A digital signature is the signing of a message hash. A variable-length message is transformed into a fixed length hash (or digest), using a hash algorithm. This hash is then encrypted with the sender's private key as described above, creating the digital signature. The message is sent along with the digital signature so the receiver can verify the message.

Through the use of encryption and digital signatures, a PKI can provide four basic security services.

- **Confidentiality** –the protection of information from unauthorized disclosure, provided through encryption.
- **Integrity** – the protection of information from unauthorized and undisclosed modification, provided through digital signatures.
- **Non-repudiation** – proves the association of data with an individual such that the individual can not deny this or claim modifications were made to the data, provided through digital signatures.
- **Authentication** – the process of verifying and ensuring an individual's identity, provided through digital signatures.

It is this last piece that we are most concerned with - authentication. While a PKI can be thought of as an arrangement binding public keys to identities, it is also the actual infrastructure needed for this arrangement to take place. A public key is issued to the user in the form of a certificate, signed by the Certificate Authority (CA). The CA is the trusted third party who can facilitate interactions between two parties that otherwise would not be trusted. A PKI is typically set up in a tree hierarchy, with the Root CA at the top of the tree. There are zero or more levels of intermediate certificates, followed by the end-entity certificates at the bottom level. An intermediate certificate is a subordinate certificate to the root CA whose purpose is to issue and sign end-entity certificates.



PKI/CAC Authentication in Department of Defense

In the case of DoD, there are two main root CAs – DoD Root CA2 and DoD Class 3 Root CA. Each of those, in turn, have issued in the range of 20-30 intermediate certificates. They are usually broken up in a way that about half are named CA-# and the other half EMAIL CA-#. Those intermediate certificates have issued millions of end-entity certificates. The end-entity certificates for users are stored on a smart card, known as a Common Access Card (CAC) within the government. The CAC is the identification card issued for government employees and contractors, both in terms of physical identification and authentication to computers and networked systems within DoD.

The CAC contains three certificates – a Signature Certificate, an Encryption Certificate and an ID Certificate. The ID certificate is issued by the CA-# intermediate cert and is used to identify the owner. This can be used for CAC logon, i.e. Authentication. The Signature and Encryption Certificates are both issued by the EMAIL CA-# intermediate cert. The Signature certificate can also be used for CAC logon.

Each certificate contains a number of fields holding different pieces of information. Those main fields are as follows,

- **Version** – identifies the X5.09 standard applied to the certificate while also indicating which fields can be expected (based on which standard).
- **Serial Number** – a unique number assigned to the cert by the issuing CA which identifies it within the PKI.
- **Signature Algorithm** – the encryption algorithm used to signed the certificate
- **Issuer** – the name of the CA that issued the certificate
- **Valid From** – the start date for the certificate after which it is valid
- **Valid To** – the end date for the certificate prior to which it is valid
- **Subject** – the DN of the entity whose public key the certificate identifies
- **Public Key** – the actual public key of the entity
- **Extensions** – optional extensions providing additional information

The smartcard (CAC) is just one of the many pieces that are needed for the authentication to take place. Those pieces include the smart card, a card reader, middleware, an application and a validation server.

- The CAC contains the certificates used for the security services.
- The card reader is what allows the card to interface with the middleware.
- The middleware is the software which allows the card to interact with the Operating System and, ultimately, the application.
- The browser is the application used to communicate with the validation server.
- The validation server handles authentication by verifying the client certificate and allows/denies access accordingly.

The middleware handles the reading of information off the smart card. After insertion of a smart card to the card reader, the middleware will prompt for a user's PIN code, needed for credential extraction. This provides two-factor authentication as it requires something you have (smart card) and something you know (PIN). At this point, the middleware can decrypt the credentials on the card, extract them and pass them to applications for use as needed.

PKI Validation

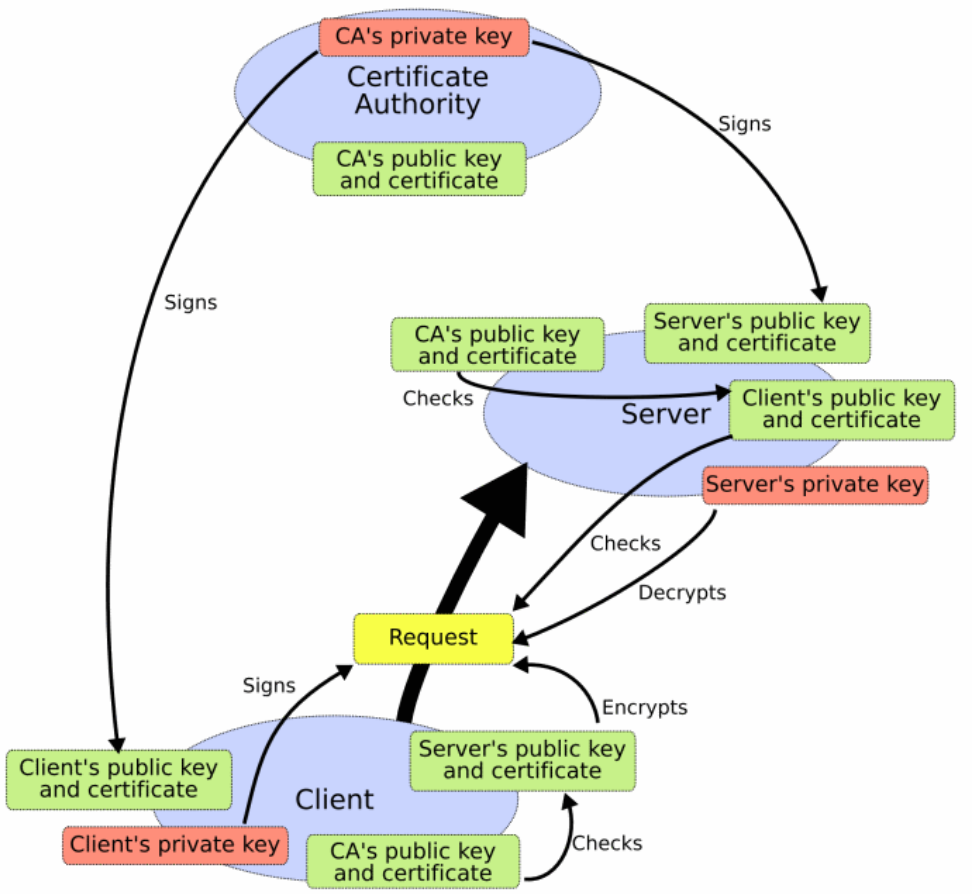
When a client application connects to a server and the server requests credentials of a particular CA group of client certificates, then the extracted credential will be sent by secure SSL channel to the server which established an SSL handshake with a browser/client initiated connection. The process for SSL handshake validation with a PKI solution is based on the validity of the client (end-entity) certificate. If the certificate is not valid, then the SSL handshake won't be established.

After the Hello exchange between the client and server and hash key exchange, the server will send server certificate (if it has one). If the server's SSL certificate is not self-

signed, then the client will also request the certificate chain related to the server's certificate. A certificate chain is a sequence of certificates where each certificate is signed by the subsequent certificate. The last certificate in the chain is normally a self-signed certificate. The root CA in a PKI hierarchy is always self-signed and is thus at the top of the chain. Because the root CA is the trusted third party, the server certificate is valid if the client can validate each step in the chain.

The client application must also have a cryptography engine in order to properly validate a server's SSL certificate for secure communication. Once the application (browser) properly validates the server's certificate, the server will request client certificates based on requests built from the prepared content chain on server side. The chain can contain multiple root certificates. So, the server can request all client certificates related to one or more root certificates from its chain.

Based on this request, the client knows if it can or can not send its client certificate to the server. If the client certificate is from the requested root tree, but there are some missing intermediate certificates from the pre-created chain of the server, then the server will request the entire chain related to the received client certificate. If the client certificate is validated on the server side than SSL handshake will be established and all traffic from this point is encrypted inside SSL channel between client and server.



PKI Validation Process

In order to verify the client certificate, the validation server must be able to verify the certificate chain up to a trust point that it has in common with the client certificate. Verifying the chain is the process of ensuring that it is well-formed, valid, correctly signed and trustworthy. There are three steps to the process, with each one starting with the certificate at the bottom of the chain (client certificate) and working its way up to the root certificate at the top.

1. It checks the certificate signature and verifies it using the public key of the issuing certificate. The client can send only the client certificate, or it can send the entire chain, to the validation server. If the client sends only its client certificate, then the validation server must retrieve the higher level certificates and rebuild the entire chain. For this reason, the validation server will often have the PKI hierarchy loaded

into the system. In the DoD example, typically both root CAs (Root CA2 and Class 3 Root CA) and all of their intermediate certificates will be loaded for the purpose of building the necessary certificate chains for client certificate validation.

2. It confirms that the certificate is still valid and has not expired. Time validation is based simply on the time in the validation server, so it is very important to properly maintain the system time on the validation server.
3. It checks that the certificate has not been revoked (is no longer valid) by looking in the Certificate Revocation List (CRL) or performing an On-line status check. All Certificate Authorities must keep a list of certificates that have been revoked (known as the CRL) so valid certificates can be properly verified. The certificates are represented by their Serial Number, which is one of the fields of the certificate.

The size of the CRL depends on the quantity of signed certificates by the parent CA. In the case of DoD, each list can be up to 20MB+. Each CRL has an expiration time. The information included in list can be trusted up until that time. The CRL has to be renewed after expiration date and all validation processes should fail if working with an expired CRL. In this situation, the client certificate has to be revoked. It is not important if this client certificate was valid at this point or not because it was unable to properly verify against a valid CRL that the certificate was not revoked.

There are three methods available on the validation server to check that the certificate has not been revoked. Two of them require a TCP/IP connection out of validation server to an authority server while the other requires keeping the CRLs locally on the validation server.

- **CRL list uploaded to local machine**

  This method requires allocation of local storage space large enough to store the needed CRLs. As mentioned previously, the size of each CRL can be rather large depending on the quantity of certificates issued by the CA, so it is not trivial. Also, it is very important to refresh the CRL before the expiration time of the list to keep an actual CRL on the validation server. In addition, the administrator has to check if

the CA released updates to the CRL where some new certificates were revoked. Situations like this are very critical because emergency revoked certificates in CRL can be safety issue for validation machine. Because of this, there is significant administrative overhead to this method.

The validation process in this method only extracts the serial number of received certificate and it will check revocation status related to the serial number inside a locally stored CRL.

- **LDAP server validation**

  This method uses an LDAP server as a collector of actual CRLs. During the validation process, the validation server will extract credentials from the received client certificate. One of the fields of the certificate is the CRL Distribution Point, which is a link to the LDAP server which keeps the actual CRLs. The validation server must download the entire CRL from the LDAP server. This method covers the critical, administrative issues with locally stored CRLs mentioned previously, but is time consuming.

- **OCSP server validation**

  OCSP (Online Certificate Status Protocol) is a protocol used for obtaining the revocation status of a certificate. It was created as an alternative to CRLs due to some of the issues mentioned in the two methods above. In this case, information about the OCSP server (known as a responder) is stored as a field in the certificate. The validation server sends a request with the Serial Number of the certificate to the OCSP responder and receives a response back with the certificate is good or revoked. Requests to the OCSP responder can be sent via http or https protocol.

Once the client certificate is validated, the user is authenticated and can log in to the validation server. For the purpose of local authentication to the machine, the Distinguished Name (DN) of the owner of the certificate is extracted and is used as the login name on the local machine, where a password was not required.

To define a group of users who are allowed to authenticate to the local machine via a client certificate, there is a registration process. The first time that a client certificate is validated, it is sent to a pending status where an administrator of the local machine must approve/disapprove the user. The user can not log in to the machine until the administrator approves him, at which point an account is created on the local machine with the login name matching the DN on the certificate. At this point, the user acts just like a local account on the validation server, and policy can be assigned to that user.